УДК 004.056.5

Застосування принципу математичного більярду Сіная для передачі шифрованної інформації

Собінов О.Г., викладач,
Центральноукраїнський національний технічний університет, м. Кропивницький

Сьогодні немає потреби говорити про важливість захисту інформації в комп'ютерних системах (КС). Як державні, військові та комерційні КС, так і приватні потребують захисту інформації. В наш час існує велика кількість засобів та методів криптографічного захисту.

В даній роботі, нас будуть цікавити не стільки класичні КС, скільки системи побудовані на ARM мікроконтролерах (ARM МК). Так, наприклад, для підвищення захищеності своїх додатків компанія STMicroelectronics випустила програмний пакет X-CUBE-CRYPTOLIB. В цьому пакеті реалізовані найбільш популярні алгоритми захисту даних для всієї родини ARMMK, навіть для тих, які не мають у своєму складі апаратної підтримки криптографії [1].

Крім того STMicroelectronics випустив ARMMK - STM32F405 і STM32F407 та STM32F415 і STM32F417, в які вбудовано crypto/hash-процесор. Цей процесор забезпечує апаратне прискорення AES 128, 192, 256, Triple DES, HASH (MD5, SHA-1). Пропускна здатність шифрування по AES-256 досягає 149,33 Мбайт/с. Як бачимо, зростання потужності (швидкодії МК), та збільшення їх використання в IT надає нові можливості, які пов'язані з забезпеченням захисту даних [2].

В [3] запропоновано простий метод шифрування, що побудовано на теорії математичного більярду (МБ). Цей метод відрізняється простотою реалізації і може слугувати прототипом створення окремої незалежної системи індивідуального криптозахисту POINT-TO-POINT.

В даному випадку на засадах МК створюються два програмно залежних прилади. В кожному з них реалізується алгоритм математичного більярду Сіная [4] (рис. 1).

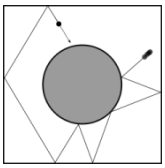

Рисунок 1 – Математичний більярд Сіная

Особливостями запропонованого алгоритму є:

- в системі МБ використовується три об'єкти – дві кульки малого

радіусу ***r*** і "шайба" радіусу ***R<L*** (довжина сторони більярда);

- для кожної пари пристроїв встановлюються індивідуальні початкові координати об'єктів ***x,y*** та швидкості (***dx, dy***);

- відкритий ключ генерується RTC і є унікальним при кожному сеансі передачі як в одну так і іншу сторону;

- відкритий ключ передає інформацію про зміщення встановлених даних на деякі малі дискретні дані.

Якщо в якості ключа використовувати значення поточної дати та часу передачі і у цьому ключі передавати послідовно значення, то:

- dx_1, dx_2,dx_p, dy_1, dy_2,dy_p – зміщення координат кульок та шайби на більярдному столі від встановлених у програмній парі МК;
- V_{1x}, V_{2x}, V_{1y}, V_{2y} – швидкості (напрямок руху кульок);
- dR_{xy}– інертність шайби;
- r_1, r_2, R_p– радіуси кульок та шайби.

Як бачимо, відкритий ключ складається з 14*N, де N – розрядність МК. Для 16 розрядного МК ключ буде мати довжину 14*16=224 біти, для 32 розрядного МК відповідно 14*32=448. Для збільшення ефективності секретності для кожної пари POINT-TO-POINTМК початкові значення, що передаються з відкритим ключем, можна встановити окрему послідовність вхідних параметрів, що складе 14!=871782911200 комбінацій. Таким чином можна забезпечити ще один секретний ключ, який притаманний тільки відповідній парі МК.

Технічно шифрування/дешифрування на принципі МБ Сіная може полягати в простому виконанні операції XOR між сигналом та ключем.

Враховуючи вищесказане і те, що кожний згенерований псевдовипадковий ряд (ключ шифрування) в системі більярда Сіная є ергодичним [5], можна вважати, що хаотичність створена системою не дозволяє відкрити переданий шифр будь-якої довжини за прийнятний час.

Список літератури

1. Новости электроники №10 (156), 2016 г. Информационно технический журнал. Учредитель – ООО «КОМПЭЛ».

2. Новости электроники №6 (44), 2012 г. Информационно технический журнал. Учредитель – ООО «КОМПЭЛ».

3. Собінов О. Г. Простий генератор псевдовипадкової послідовності / О. Г. Собінов // Інформаційні технології та комп'ютерна інженерія : зб. тез доп. наук.-практ. конф., м. Кіровоград, 4 груд. 2014 р. – Кіровоград: КНТУ, 2014. – С. 184.

4. Гальперин Г.А., Земляков А.Н. Математические бильярды. Бильярдные задачи и смежные вопросыматематики и механики – М.: Наука, 1990. – 288 с.

5. Ганапольский Е.М. О природе квантового хаоса в рассеивающей бильярдной К-системе / Е. М. Ганапольский // Доповіді Національної академії наук України. - 2012. - № 3. - С. 85-91.